

Creating and managing network blueprints using the Network Designer

You use the Network Designer workspace to create network blueprints. A network blueprint is a topology blueprint used to carve out logical network isolations from physical devices. You can create simple network blueprints that set up a public-facing subnet to host a web application, or more complex blueprints that connect public cloud resources in a private, non-Internet facing corporate data center.

Note

Currently, the Network Blueprint workspace applies to Amazon Web Services (AWS) environments only.

This topic describes how to use the Network Designer to create network blueprints. It includes the following sections:

- [Before you begin](#)
- [Creating a new network blueprint](#)
- [Managing network blueprints](#)
- [Blueprint example](#)
- [Where to go next](#)

The following BMC Communities video (6:46) describes how to use IP address resources in network blueprints using BMC Network Automation. The blueprints can then be imported into BMC Cloud Lifecycle Management.



▶ <https://youtu.be/CQD6Si3wZa4>

Before you begin

Ensure that you have completed the following tasks:

- If you are creating a blueprint for an AWS environment, ensure that you:
 - [Configure the Amazon Web Services provider type](#)
 - [Configure user credentials for Amazon Web Services workloads](#)
- If you want your enterprise IP address management (IPAM) solution to manage the IP addresses for the servers in an AWS or Azure environment, enable IP management in BMC Network Automation and BMC Atrium Orchestrator.
- If you want your enterprise domain name system (DNS) solution to provide the IP addresses for the servers in an AWS or Azure environment, configure BMC Atrium Orchestrator for DNS registration.
- Follow the standard guidelines to add a DNS to your network.
- Plan your network blueprint. Because of the many different ways you can create a network blueprint, you might not need each of the major steps provided in this topic. Plan your blueprint, and then follow the procedures you need to create the blueprint you have planned. You can create network blueprints that include some or all of the following objects, in whatever numbers you choose:
 - Internet
 - Networks
 - Gateways (for the Internet or VPN)
 - Perimeter and distributed firewalls
 - Load balancers

Creating a new network blueprint

The following sections describe the tasks you must perform to create a network blueprint.

To create a network blueprint

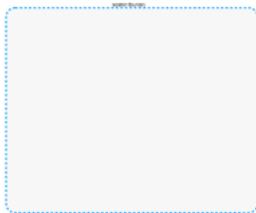
Follow this procedure to create a new network blueprint.

1. From the BMC Cloud Lifecycle Management Administration Console, click the vertical **Workspaces** menu on the left side of the window and select **Network Designer**.



2. In the Network Designer workspace, click **Create New**.

The Network Designer canvas is displayed. The following icons indicate the available components you can use to build your network blueprint.

Icon	Description
	Isolation boundary - Represents the scope of the logical hosting environment being modeled by the network blueprint. Entries in the route table are managed automatically based on connections drawn between networks in the network blueprint. In AWS, the Isolation Boundary represents the Virtual Private Cloud (VPC). Note that within every AWS VPC, there is an implicit router responsible for traffic between all VPC subnets.
	Internet - Creates an object representing the Internet, which can be configured to allow nodes inside the Isolation Boundary to access nodes outside of it using the Internet. By default, the Internet object has a value for the address range that represents the entire addressable space. However, a more restrictive (single) address range can be specified, perhaps representing a particular external network (when not using a VPN tunnel).
	Network - Represents a contiguous address range to which workloads can be attached. At least one network must be included in the Isolation Boundary. A network can be public or private, and can be configured for Network Address Translation (NAT).

In AWS, a network represents a VPC subnet, designated as Public or Private.

Note

Routing for networks is driven by an implicit router (which is not represented in a network blueprint). Routing rules are managed by the Layer 3 connectivity lines you draw between networks, which are then applied to the routing table(s) for the networks.



Edge gateway - Provides egress from and ingress into the Isolation Boundary, either to the Internet or to a corporate network using a VPN tunnel (based on settings). Place this object within the Isolation Boundary.

For an AWS environment, this object represents an Internet Gateway or a VPN Gateway object within the VPC, depending on the type specified.



Enterprise gateway - Represents the enterprise end of a VPN tunnel. Place the gateway outside the Isolation Boundary and connect it to an Edge Gateway within the Isolation Boundary to model a VPN tunnel.

You configure the settings of the VPN by selecting the connection line on the canvas. Attach a subnet to the gateway to represent address ranges in the enterprise network that will have access to subnets within the Isolation Boundary.

For an AWS environment, this object represents a Customer Gateway.



Perimeter firewall - Represents a logical, stateless, edge firewall service with visibility into network traffic (as opposed to workload-specific traffic).

For an AWS environment, a single Perimeter Firewall object represents (potentially multiple) AWS Network ACLs.



Distributed firewall - Represents a logical, stateful distributed firewall service with visibility into workload-specific traffic (as opposed to network traffic).

For an AWS environment, a single Distributed Firewall object represents (potentially multiple) AWS Security Groups.



Load balancer - Represents a logical load balancer, which distributes traffic across multiple server workloads for scalability and redundancy. These objects are connected on the:

- Server side to subnets, where the server workloads reside
- Client side to subnets (or edge gateways) from which clients connect to the load balanced service

In AWS, these objects do not represent an Elastic Load Balancer (ELB), but are Load

Balancer Pools in service blueprints that actually correlate to AWS ELBs. AWS obviates the component that equates to an on-premise logical load balancer. However, BMC Cloud Lifecycle Management still requires the creation of these logical load balancers to:

- Identify Network Containers and Logical Hosting Environments that allow load balancing services (bronze versus silver level containers)
- Govern the networks to which the Load Balancer Pools (or ELBs, in the case of AWS) may be connected during service instance provisioning.



Domain Name System – Represents a domain name system (DNS), which is used to resolve the host name of a server.

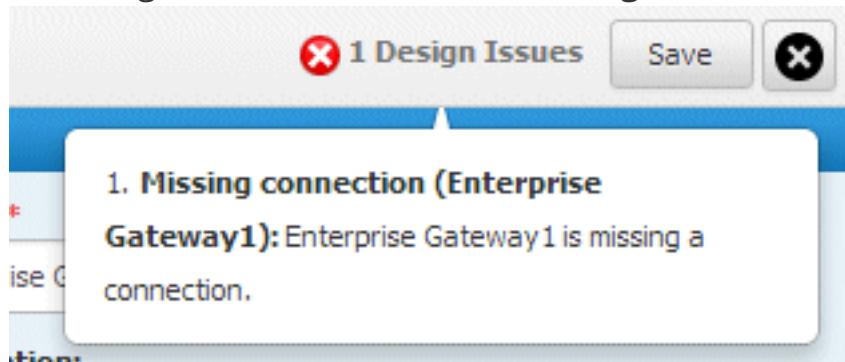
Servers provisioned in AWS are registered in the DNS that exists in the on-premises data center by using their public or private IP addresses. The servers are also enrolled in BMC Server Automation by using the same host name that was used to register in the DNS. This configuration ensures that BMC Server Automation can communicate to the servers using their *host names* instead of IP addresses. Using host names allows for the public IP addresses of such servers to change without affecting their connectivity with the BMC Server Automation server.

Notes about DNS:

- DNS support is provided on the isolation boundary and at the network level.
- A DNS cannot connect to more than one data center or network.
- Only one DNS can be connected to one network or isolation boundary.
- The DNS you enter in a network blueprint or when creating a logical hosting environment (LHE) cannot be modified. If you want to modify a DNS, you must delete the existing DNS entry first. In the network blueprint, you can modify the DNS details anytime. For the LHE level, you must delete existing DNS details and then, without saving, enter new DNS details in **DNS Registration Details** tab and at the LHE network level.
- In a network blueprint, you cannot add more than one DNS for more than one network. (For example, Network 1 includes DNS 1, and Network 2 include DNS 2.) But you can add a different DNS when creating the LHE at the network level.
- At the LHE level, you can change the **Enable DNS Registration** check box (on a Create or Modify Logical hosting environment dialog box) even after workload is running on that LHE, but you *cannot* change the **Enable External DNS** check box if workload is running on the network.

For information about creating an LHE (also called a logical data center) as mentioned in the notes above, see [Creating a Logical Data Center for Amazon Web Services](#).

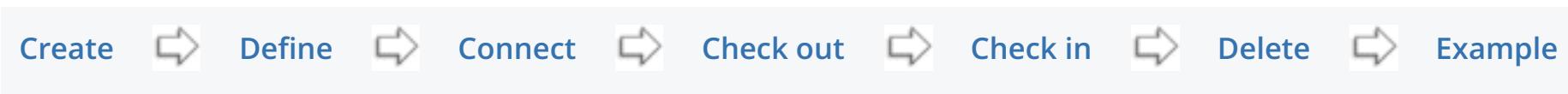
3. [Add, define, and connect components](#) in the network blueprint. Use either of the following methods to add a network component on the canvas:
 - a. Click the network component icon from the component list on the left; the network component icon appears on the canvas.
 - b. Drag a network component icon from the component list and drop the component icon to the desired location on the canvas.
4. Ensure that the icons are positioned in the desired location on the canvas.
5. [Draw connection lines](#) between the objects.
6. Check the **Design Issues** label to ensure that the network blueprint has been properly configured. If there are design issues, hover over the **Design Issues** label to see a list of the issues.



You can save a blueprint with Design Issues, but will not be able to check it in until the issues are resolved.

7. Click **Save**.
8. Enter a unique name for your blueprint to describe the network.
9. Click **Create**.

Use the navigation bar below to jump to different sections in the topic:



[Back to top](#)

To add and define network blueprint components

The following table describes how to add and define the various components to a network blueprint. To see the fields used to define a component, select the component so that it has a thick border (not a dotted-lined border).

Component	Procedure
Isolation Boundary	<p>Use this option to create the boundary for the logical hosting environment.</p> <p>Details</p> <p><input checked="" type="checkbox"/> Enable External IPAM <small> ⓘ</small></p>

Internet

The screenshot shows a 'Details' tab for creating an 'Internet' object. It includes fields for 'Name' (set to 'Internet'), 'Description', 'Network Address' (set to '0.0.0.0'), 'Network Mask' (set to '0.0.0.0'), and 'Tags' (with an 'Add tag...' button).

Use this option to create an object representing the Internet .

1. Enter a unique **Name** for the internet connection.
2. Optionally, enter a **Description**.
3. Enter the IP address in the **Network Address** field.

Along with Network Mask, the Network Address identifies the address range that workloads in the Isolation Boundary can access. By default, the Internet object has a value for the address range (0.0.0.0/0.0.0.0) which represents the entire addressable space. However, a more restrictive (single) address range can be specified, perhaps representing a particular external network (when not using a VPN tunnel).
4. Enter a **Network Mask**. The default value is 0.0.0.0. Enter a range of IP addresses to limit Internet access to a specific range of addresses.

Along with Network Address, the Network Mask identifies the address range that workloads in the Isolation Boundary can access. The default value (0.0.0.0/0.0.0.0) allows for the entire addressable space, but a more narrow range could be used to restrict to specific external network's address range.
5. Optionally, add a **Tag**.

Use a tag value such as "internet" or "external" for the Internet object. This tag should match the tag value on the load balancer pool object in Service Blueprints. For more information about using tags, see [Creating tag groups and tags](#).

Network

The screenshot shows a 'Details' tab for creating a 'Network' object. It includes fields for 'Name' (set to 'Network1'), 'Description', 'Network Address' (set to '192.168.1.0'), 'Network Mask' (set to '255.255.255.0'), and several checkboxes for traffic types: 'Public' (unchecked), 'Use Default Route Table' (checked), 'Use NAT' (unchecked), 'Serving Customer Traffic' (unchecked), 'Serving Management Traffic' (unchecked). There is also a 'Tags' section with an 'Add tag...' button.

Use this option to create a subnet. You can add one or more subnets.

1. Enter a unique **Name** for the subnet.
2. Optionally, enter a **Description**.
3. Enter a **Network Address**.

Along with Network Mask, the Network Address identifies the IP Address range of the subnet.
4. Enter a **Network Mask**. Along with the Network Address, the Subnet Mask identifies the IP Address range of the subnet.

In AWS, address ranges for VPCs can be no broader than 255.255.0.0; therefore, the network ranges must fit within that scope.
5. Select from the following options:
 - a. **Public** - Select if the network is public-facing.

In this case, a route is added in the route table allowing outbound traffic through the Edge Gateway. If this option is not selected (indicating a private network), only a local route is added.

Network with load balancer

The screenshot shows a 'Details' tab for creating a 'Network' object with a load balancer. It includes fields for 'Name' (set to 'Network1'), 'Description', 'Network Address' (set to '192.168.1.0'), 'Network Mask' (set to '255.255.255.0'), and several checkboxes for traffic types: 'Public' (unchecked), 'Client' (unchecked), 'Server' (checked), 'Use Default Route Table' (checked), 'Use NAT' (unchecked), 'Serving Customer Traffic' (unchecked), 'Serving Management Traffic' (unchecked). There is also a 'Tags' section with an 'Add tag...' button.

Network with DNS



In AWS, this corresponds to descriptions of Public and Private subnets in the Amazon VPC creation wizard.

- b. **Client** - Select this option to indicate that this network will contain server workloads that will make client requests of a load balancer connected to this network. For example, if this network will house web servers that will initiate connections to a load balanced application server farm, then select this option.

The option is displayed only if the network is connected to a load balancer.

- c. **Server** - Select this option to indicate that this network will contain servers that will be load balanced by a load balancer connected to this network. For example, select this option if this network will house web servers that make up a load.

The option is displayed only if the network is connected to a load balancer.

Note: For AWS environments, if you do *not* want to load balance specific networks, do *not* select the **Server** check box (by default, it is selected); otherwise, the networks will be load-balanced by *all* available load balancers in the logical hosting environment.

- d. **Use Default Route Table** - Select this option to use the common, default route table shared by other networks in this network blueprint.

A network must have exactly one route table, which specifies the allowed routes for outbound traffic leaving the network. Networks might share a common route table or they might have their own. Use of the default (common) route table is primarily relevant to *public networks*, as private networks should not use the default route table. Entries in the route table are managed automatically based on connections drawn between networks in the network blueprint.

- e. **Use NAT** - Select this option to specify that this network needs Network Address Translation (NAT) when accessing network endpoints outside the isolation boundary. A network using NAT should not be marked public (it must be a private network). In AWS, this option creates a NAT translator, which assigns dynamic public IP addresses to associated instances workloads in private networks in the VPC, as they access external endpoints.

- f. **Serving customer traffic** - Select this option to indicate that this network will be used for *customer* traffic (for example, general web or database access), as opposed to *management* purposes

(for example, by BMC Server Automation). Some networks may be used for both.

- g. **Serving management traffic** - Select this option to indicate that this network will be used for *management* purposes (for example, by BMC Server Automation), as opposed to *customer* traffic (for example, general web or database access). Some networks may be used for both.
- h. **Enable External DNS** - Select this option to enable DNS registration, which enables you to manage servers through BMC Server Automation.

This option is displayed only when you add a Domain Name System and connect it to the isolation boundary or at the network level. Then, the option is selected by default.

If you do not want your server to be added in the DNS, clear the **Enable External DNS** check box.

If you are adding an additional network to your network blueprint and DNS is applied at the LHE level, the **Enable External DNS** check box is not automatically selected on the network blueprint. You must select the check box.

6. (*Optional*) Set the **Tags** that are referenced by service blueprints to place workloads in this network.
7. For example, if this network (along with others) is intended to host web servers, you might specify **Web** as the tag. For more information about using tags, see [Creating tag groups and tags](#).

In AWS, the **TARGET_AWS_ZONE** tags (provided by default) are used to identify the availability zone in which each network is created. **TARGET_AWS_ZONE** tags can be specified here in the network blueprint, or be supplied when VPC instances are created from a network blueprint. If no **TARGET_AWS_ZONE** tag is specified, then BMC Cloud Lifecycle Management will choose an arbitrary Availability Zone. Additionally, more generic tags may be used to identify region-neutral Availability Zone distinctions, such as "AZ-1" and "AZ-2".

This method allows service blueprints to designate that two web servers are placed in separate Availability Zones without needing to know what region or specific Availability Zones are in use in a particular VPC. Furthermore, these more generic tags can be used for direction on specific Availability Zones that should be selected during VPC instance creation from the network blueprint.

Details

Name: *	Edge Gateway1
Description:	
Gateway Type: <input checked="" type="radio"/> Internet Gateway	<input type="radio"/> VPN Gateway

1. Enter a unique **Name** for the gateway.
2. Optionally, enter a **Description**.
3. Set the **Gateway Type** to indicate whether this Edge Gateway is intended to connect to an **Internet Gateway** (public traffic) or to an enterprise **VPN Gateway** (private traffic).

Enterprise gateway

Details

Name: *	Enterprise Gateway1
Description:	
<input checked="" type="checkbox"/> Static Routing <small>(i)</small>	
IP Address: *	

Use this option to create the enterprise end of a VPN tunnel.

1. Enter a unique **Name** for the gateway.
2. Optionally, enter a **Description**.
3. Select the routing option to determine the type of routing for the Enterprise Gateway:
 - a. Select **Dynamic Routing** to indicate routing via Border Gateway Protocol (BGP).
 - b. Enter the **IP Address** of the VPN server.
 - c. Enter the **Autonomous System Number** (ASN).

If you prefer *static routing*, clear the **Dynamic Routing** check box, and specify the **IP Address** of the VPN server.

Perimeter firewall

Details

Name: *	Perimeter Firewall1
Description:	
Firewall Interfaces: <small>(i)</small>	

Firewall Interfaces:

Name	Network	Direction

This option enables you to add an edge firewall service with visibility into network traffic (as opposed to workload-specific traffic). Perimeter firewalls typically provide network-level security.

In AWS, this option represents using a Network ACL.

1. Enter a unique **Name** for the firewall.
2. Optionally, enter a **Description**.
3. To add a firewall interface that defines interfaces on the firewall, each of which secures a network, complete the following steps:
 - a. Click the **Add** icon .
 - The Firewall Interface - New panel is displayed.
 - b. Add a name for the firewall interface.
 - c. Optionally, add a description.
 - d. Select the target network being secured by this firewall interface.
 - e. From the drop-down list, select the direction of the traffic (**Inbound**, **Outbound**, or **Direction Agnostic**) that is being secured by subsequent firewall rules. You add rules via provisioning of service instances with network path details or via

the ad-hoc [Manage Firewall Rules](#) or [Manage Network Path](#) panels).

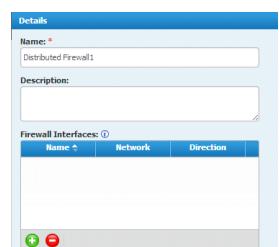
Note

The cloud administrator must open the following ports in the Network ACLs to enable communication with the BMC Server Automation RSCD Agent:

- Inbound connection: Open the RSCD Agent port (by default, port 4750) for TCP communication
- Outbound connection: Open all the ports for TCP communication (ports 1 – 65535 , since the firewall is stateless)

You can create these firewall rules using the ad-hoc [Manage Firewall Rules](#) panel available in the Resources workspace. These ports must be opened to ensure the RSCD agent on the provisioned instance is able to communicate with the BMC Server Automation server to enable the creation of security groups, as defined in the Service Blueprint.

Distributed firewall



This option enables you to add a distributed firewall service with visibility into workload-specific traffic (as opposed to network traffic).

In AWS, this object represents a Security Group.

1. Enter a unique **Name** for the firewall.
2. Optionally, enter a **Description**.
3. To add a firewall interface that defines interfaces on the firewall, each of which secures a network, complete the following steps :
 - a. Click the **Add** icon . The Firewall Interface - New panel is displayed.
The Firewall Interface - New panel is displayed.
 - b. Add a name for the firewall interface.
 - c. Optionally, add a description.
 - d. Select the target network being secured by this firewall interface.
 - e. From the drop-down list, select the direction of the traffic (**Inbound**, **Outbound**, or **Direction Agnostic**) that is being secured by subsequent firewall rules. You add rules via provisioning of service instances with network path details or via

the ad-hoc [Manage Firewall Rules](#) or [Manage Network Path](#) panels).

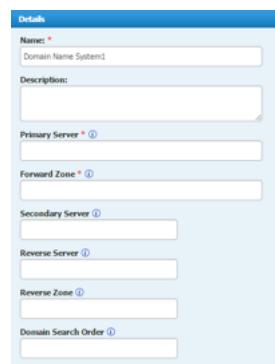
Load balancer



This option enables you to distribute traffic across multiple server workloads for scalability and redundancy.

1. Enter a unique **Name** for the load balancer.
2. Optionally, enter a **Description**.

Domain Name System



Use this option to enable DNS registration.

1. Enter a unique **Name** for the DNS.
2. (*Optional*) Enter a **Description**.
3. In the **Primary Server** field, enter the Primary DNS server name.
4. Enter the **Forward Zone**.
This DNS zone is where the host-name-to-IP-address relations are stored (for example, **calbro.com** or **production.calbro.com**).
5. (*Optional*) Enter a **Secondary Server** name.
6. (*Optional*) Enter a **Reverse Server** name.
7. (*Optional*) Enter the **Reverse Zone**. (Use the standard procedure for adding or configuring a Reverse zone.)
This DNS zone is where the IP-address-to-host-name relations are stored.
8. (*Optional*) Enter the **Domain Search Order**.

Note: If you add a DNS and connect it to an isolation boundary or a network, an **Enable External DNS** check box appears when you select the related network. (See the Network description above.)

Use the navigation bar below to jump to different sections in the topic:

[Create](#)  [Define](#)  [Connect](#)  [Check out](#)  [Check in](#)  [Delete](#)  [Example](#)

[Back to top](#)

To draw connections between components

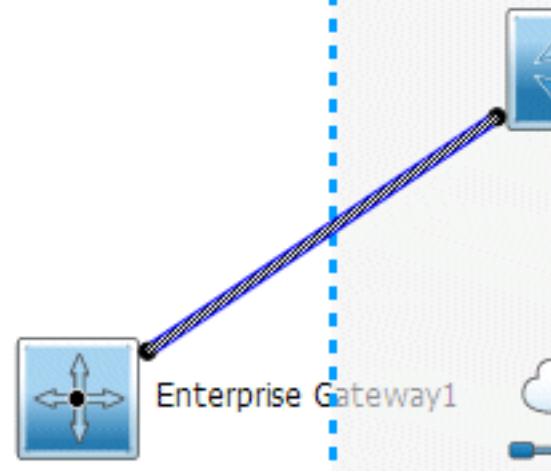
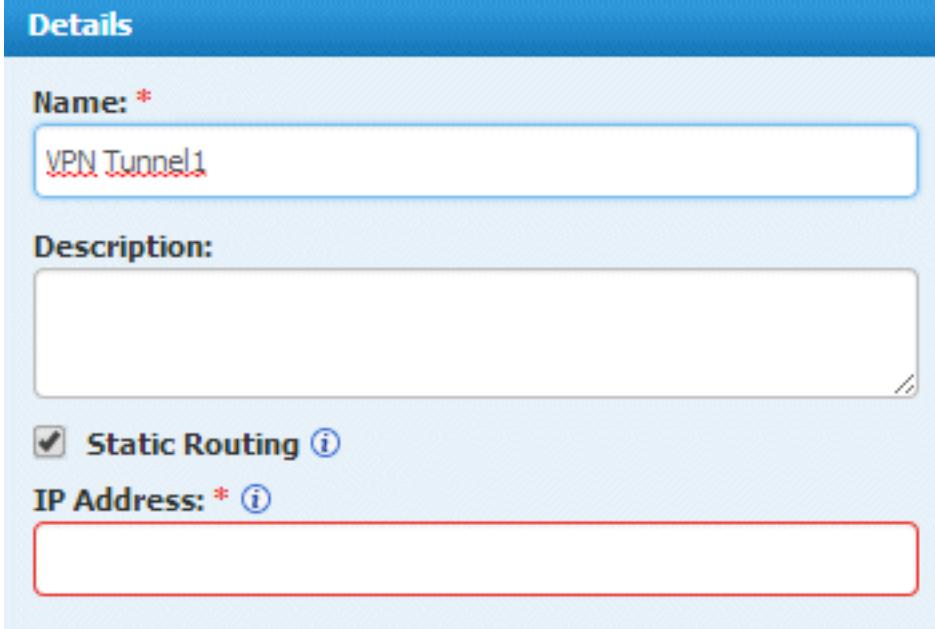
To draw a connection line:

1. Select the **Connect** icon .

2. Click and drag from the source component to start drawing a connection.

3. Release while hovering over the destination component to complete the connection.

You use the following objects to draw connections between components:

Connection type	Description	Example
Connection lines	<p>The lines that you draw between objects on the blueprint diagram.</p> <p>These lines represent connections between objects in the blueprint diagram as layer 3 routes served by an implicit router. Based on these connections, layer 3 routes are calculated and added to the route tables.</p>	
VPN connection line	<p>Draws a connection between an Edge Gateway and an Enterprise Gateway, creating a VPN tunnel.</p> <p>This connection is highlighted in blue and has properties that can be configured when selected.</p>	 

The connection line has the following configurable fields:

1. Enter a unique **Name** for the connection.
2. Optionally, enter a brief **Description**.
3. Select the routing option:
 - Select **Dynamic Routing** to indicate routing via Border Gateway Protocol (BGP), and then enter the **IP Address** and **Autonomous System Number**.

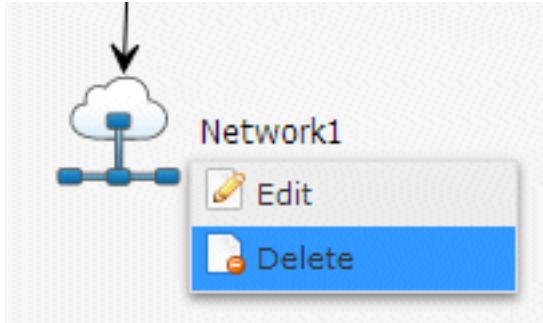
- If you prefer *static* routing, clear the **Dynamic Routing** check box, and specify the IP Address.

[Back to top](#)

To delete components and connections

To delete or remove a specific component or connection, do one of the following:

- Select the component or connection and click the **Delete** key on the keyboard.
- Right-click the selected component or connection and click **Delete** from the context menu.



Note

When you delete a component, all the connections attached to the component are also deleted.

Use the navigation bar below to jump to different sections in the topic:

[Create](#) [Define](#) [Connect](#) [Check out](#) [Check in](#) [Delete](#) [Example](#)

[Back to top](#)

Managing network blueprints

The following sections describe the various management tasks when working with network blueprints.

Network blueprint zoom controls

You can use the following icons to zoom in or out of the network blueprint.

Icon	Description
	Zooms in on the network blueprint.
	Returns the network blueprint to original size.
	Zooms out on the network blueprint.



Fits the content so that all parts of the network blueprint are visible on the canvas.

[Back to top](#)

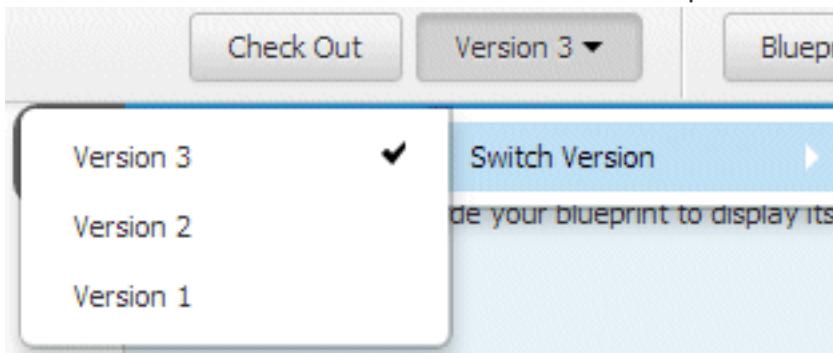
To check out and edit an existing blueprint

Follow this procedure to modify an existing network blueprint.

1. In the Network Designer workspace, select a network blueprint from the **All Blueprints** list or use the **Search** field to locate a blueprint in the list.
The network blueprint appears in view-only mode. The current version of the network blueprint is shown next to the **Check Out** label.



To work with an earlier version of the blueprint, select the version drop-down and click **Switch Version**.



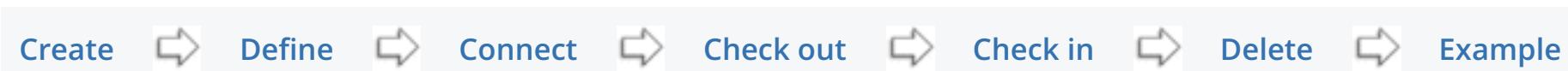
2. Click **Check Out**.

A local copy of the network blueprint is created and is listed in the **My Checked Out Blueprints** list.

3. [Add and define components](#) in the network blueprint, as needed. Use either of the following methods to add a network component on the canvas:
 - a. Click the network component icon from the component list on the left; the network component icon appears on the canvas.
 - b. Drag a network component icon from the component list and drop the component icon to the desired location on the canvas.

When you check out a network blueprint and make updates, a new version of the blueprint is created when you check it in.

Use the navigation bar below to jump to different sections in the topic:



[Back to top](#)

To check in a network blueprint

Follow this procedure when you are ready to check in the network blueprint.

1. After you finish editing a network blueprint and save it, close the Network Designer. The Network Designer workspace is displayed.
2. Check the **Design Issues** label to ensure that the network blueprint has been properly configured. If there are design issues, hover over the **Design Issues** label to see a list of the issues.



You can save a blueprint with Design Issues, but you cannot check it in until the issues are resolved.

3. Click **Working copy** and select **Check In**.

The working copy of the blueprint is removed from the **My Checked Out Blueprints** list, and a new version of the blueprint is added to the blueprint library (under **All Blueprints**).

Use the navigation bar below to jump to different sections in the topic:

[Create](#) [Define](#) [Connect](#) [Check out](#) [Check in](#) [Delete](#) [Example](#)

[Back to top](#)

To revert to a previous version

To revert a blueprint to a previous version, select an older version of the blueprint from **All Blueprints** list and save that version as the latest.

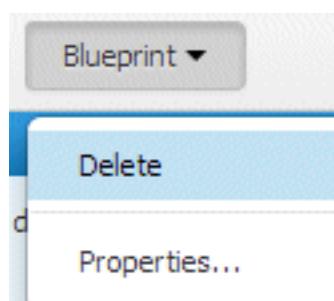
To discard or delete a network blueprint

You can discard a particular version of a blueprint, or you can delete a blueprint and all of its versions.

Task	Procedure
To discard a working copy of a network blueprint	<ol style="list-style-type: none">1. In the Network Designer workspace, click Working copy and select Discard.2. On the confirmation dialog box, click Yes. <p>The working copy of the specific blueprint version is removed from the My Checked Out Blueprints list.</p>

You can only discard a working copy of a particular version of a network blueprint, not a version of the checked-in blueprint.

To delete a blueprint



1. In the Network Designer workspace, select a network blueprint from the **All Blueprints** list or use the **Search** field to locate a blueprint in the list.
2. Ensure that the blueprint is not checked out and is not being referenced by a provisioned Local Host Environment blueprint.
3. From the Blueprint drop-down menu, select **Delete**.
4. On the confirmation dialog box, click **Yes**.

All versions of the network blueprint are deleted, and the network blueprint is removed from the **All Blueprints** list.

Use the navigation bar below to jump to different sections in the topic:

[Create](#) [Define](#) [Connect](#) [Check out](#) [Check in](#) [Delete](#) [Example](#)

[Back to top](#)

Blueprint example

In this example, you want to create a topology to run a single-tier, public-facing web application such as a blog or simple web site.

1. From the BMC Cloud Lifecycle Management Administration Console, click the vertical **Workspaces** menu on the left side of the window and select **Network Designer**.

2. In the Network Blueprints workspace, click **Create New**.

The Network Blueprints Designer is displayed, with the Isolation Boundary for the network in the center of the canvas.

3. Click the Internet icon , and enter the settings for the network.

a. Enter a **Name** for the internet connection. This example uses **Internet** as the name, and does not enter a description.

b. Enter the IP address in the **Network Address** field.

This example accepts the default for the Internet object, a value for the address range (0.0.0.0/0.0.0.0) representing the entire addressable space. However, a more restrictive (single)

address range can be specified, perhaps representing a particular external network (when not using a VPN tunnel).

- c. Enter the network mask in the **Network Mask** field.

This example uses the default **Network Mask** of 0.0.0.0, which does not want to limit Internet access to a specific range of addresses.



4. Click the Edge Gateway icon , and position the icon inside the Isolation Boundary.

- a. Enter a unique **Name** for the gateway. This example uses **Blog Gateway**.

- b. Set the **Gateway Type**. This example uses **Internet Gateway** as the gateway if for public traffic.



5. Click the Network icon , and enter the settings for the network.

- a. Enter a unique **Name** for the network. This example uses **Calbro Services**.

- b. Select **Public** to specify the network is public-facing.

- c. **Use Default Route Table** - Select this option to use the common, default route table shared by other networks in this network blueprint.

- d. **Serving customer traffic** - Select this option to indicate that this network will be used for *customer* traffic (for example, general web access or database access), as opposed to *management* purposes (for example, by BMC Server Automation). Some networks may be used for both.

- e. Leave all other options blank.



6. Click the Domain Name System icon , and enter the settings for the DNS.

Make sure that the DNS is outside of the isolation boundary.

- a. Enter a unique **Name** for the DNS.

- b. *(Optional)* Enter a **Description**.

- c. In the **Primary Server** field, enter the Primary DNS server name.

- d. Enter the **Forward Zone**.

This DNS zone is where the host-name-to-IP-address relations are stored (for example, **calbro.com** or **production.calbro.com**).

- e. *(Optional)* Enter a **Secondary Server** name.

- f. Enter a **Reverse Server** name.

- g. Enter the **Reverse Zone**. (Use the standard procedure for adding or configuring a Reverse zone.)

This DNS zone is where the IP-address-to-host-name relations are stored.

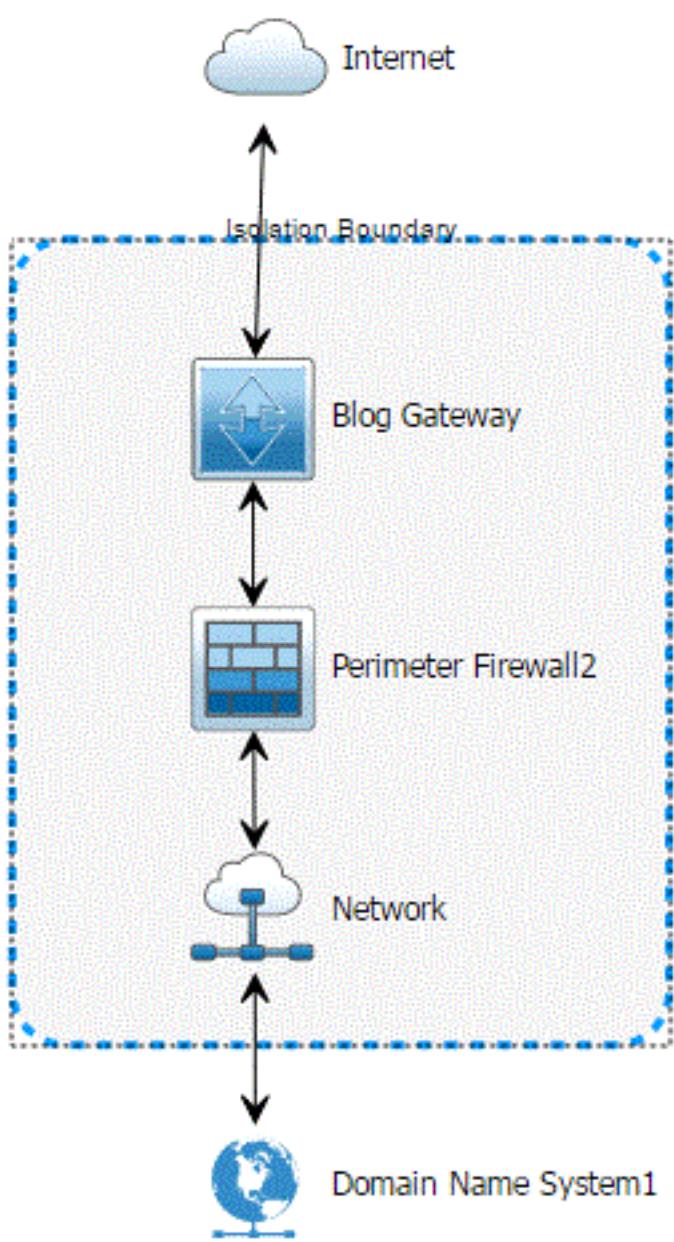
- h. *(Optional)* Enter the **Domain Search Order**.



7. Click the Perimeter Firewall icon , and enter the settings for the firewall interface. In this example,

add a firewall interface for the inbound traffic only, as the web server does not initiate outbound communication.

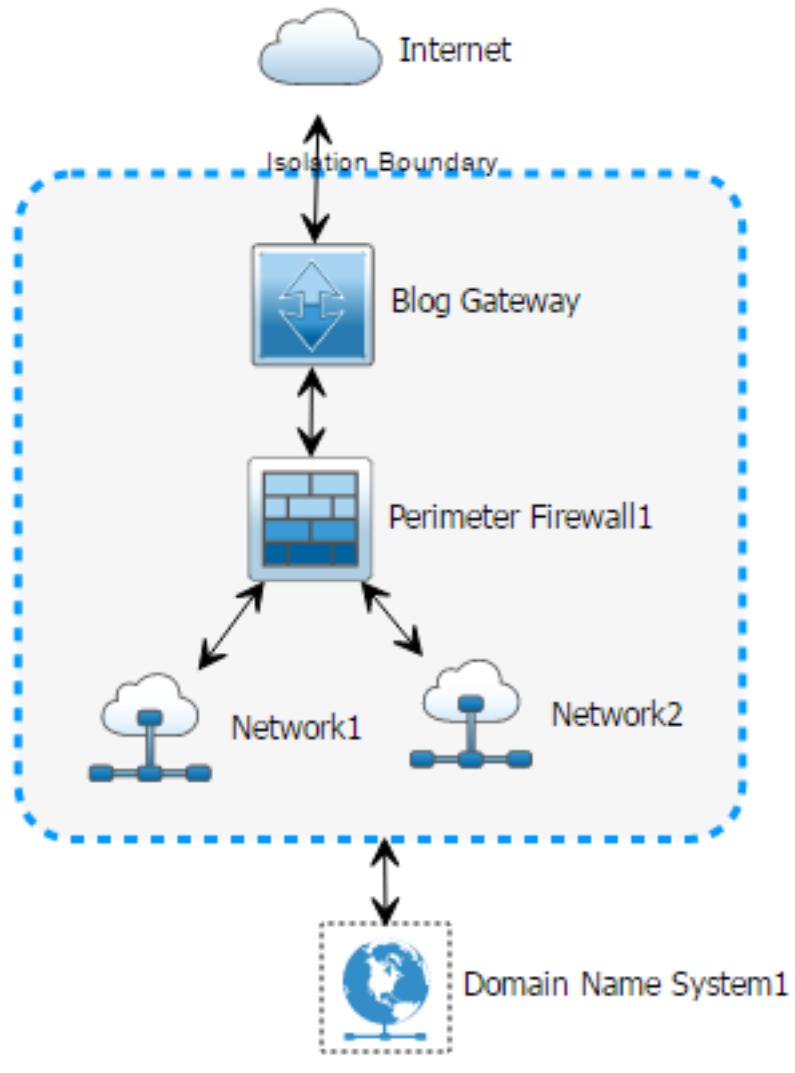
- a. Select the Network icon, and draw a connection line to the Perimeter Firewall icon. To add a firewall interface, connect the Network icon to the Perimeter Firewall icon.
 - b. Click the **Add** icon . The Firewall Interface - New panel is displayed.
The Firewall Interface - New panel is displayed.
 - c. Add a name for the firewall interface. This example uses the default, Firewall Interface 1.
 - d. Select the specific target network being secured by this firewall interface. This example uses the **Calbro Services** network.
 - e. From the drop-down list, select the direction of the traffic that is being secured. This example uses **Inbound**.
 - f. Click **OK** to add the **Firewall Interface 1**. The firewall interface information is now displayed on the Firewall Interfaces table.
 - g. Position the Perimeter Firewall inside the Isolation Boundary, between the Edge Gateway and the Network.
8. Add other connections to the components:
- a. Select the Edge Gateway icon, and [draw a connection line](#) to the Internet icon.
 - b. Select the Perimeter Firewall icon, and draw a connection line to the Edge Gateway icon.
 - c. Select the DNS icon, and draw a connection line to the Network icon.
The following example shows the network blueprint with all connections drawn.



9. Click **Save**.
10. Enter a unique name for your blueprint to describe the network. This example uses **Calbro Services Blog**.
11. Click **Close**.
The Network Designer workspace is displayed, and you will see **Calbro Services Blog blueprint** listed under **My Checked Out Blueprints** list.
12. Click **Working Copy (v0)** in the dropdown menu.
13. Click **Check In**.

Note

If you connect the DNS to the isolation boundary (as shown in the following example), then, by default, the DNS serves *all* of the networks within the boundary.



Use the navigation bar below to jump to different sections in the topic:

[Create](#) [Define](#) [Connect](#) [Check out](#) [Check in](#) [Delete](#) [Example](#)

Where to go next

You can now use this network blueprint to [create a logical hosting environment](#) onto which you can build end-user service offerings.

[Back to top](#)

Was this page helpful?

[Yes](#)

[No](#)

Comments

[Log in or register to comment.](#)

[Log in or register to comment.](#)

[Network blueprints, pods, and containers](#)

[Managing network pods](#)

© Copyright 2018 BMC Software, Inc.

[Legal notices](#)

Powered by Atlassian Confluence and Scroll Viewport

[Company](#)

[Support](#)

[Social](#)

[Search](#)

About
BMC

Upcoming
Events

Support
Central

Documentation



Communities



BMC

Blogs

Careers

On-demand
Webinars

Knowledge Downloads
Base



Facebook



Twitter

Feedback

Global
Contacts



YouTube



LinkedIn

Newsroom

Search



